NASA Information Technology Requirement

NITR 2810-20

Effective Date: March 11, 2009

Expiration Date: May 16, 2011

System and Communications Protection Policy and Procedures

Responsible Office: Office of the Chief Information Officer

Table of Contents

PREFACE

P.1 PURPOSE
P.2 APPLICABILITY
P.3 AUTHORITY
P.4 APPLICABLE DOCUMENTS
P.5 MEASUREMENT AND VERIFICATION
P.6 CANCELLATION

1.0 REQUIREMENT

1.1 System and Communication Protection Policy
1.2 Procedures

APPENDIX A. Definitions

APPENDIX B. Acronyms

APPENDIX C. Organization Defined Values for the System and Communication Protection (SC) Security Controls

Distribution:

NODIS

Change History

NITR-2810-20, System and Communication Protection Policy and Procedures

Change Number	**Date**	**Change Description**

PREFACE

P.1 PURPOSE

To provide the NASA information system and communication protection policy and procedures needed to meet the current National Institute of Standards and Technology (NIST) requirements.

P.2 APPLICABILITY

This NITR applies to unclassified information systems at NASA Headquarters and Centers, including Component Facilities and Technical and Service Support Centers. To the extent specified in their respective contracts or agreements, it applies to the NASA Jet Propulsion Laboratory, other contractors, grant recipients, or parties to agreements for information systems that they use or operate on behalf of the Agency or that support the operations and assets of the Agency.

P.3 AUTHORITY

Reference Paragraph P.3, NPR 2810.1A.

P.4 APPLICABLE DOCUMENTS

a. NPR 2810.1, Security of Information Technology.

b. NPR 1382.1, NASA Privacy Procedural Requirements.

c. NPR 1600.1, NASA Security Program Procedural Requirements.

d. NPD 2540.1, Personal Use of Government Equipment Including Information Technology.

e. Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems.

f. NIST SP 800-100, Information Security Handbook: A Guide to Managers.

g. NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

h. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.

i NIST SP 800-37, Guide for Security Certification and Accreditation of Federal Information Systems.

j. NIST SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

k. NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.

l. NIST 800-30, Risk Management Guide for Information Systems.

m. NIST 800-21, Guideline for implementing Cryptography in the Federal Government.

P.5 MEASUREMENT AND VERIFICATION

a. Annual certification of the Agency common security control, SC-1 System and Communication Protection Policies and Procedures of the System and Communication Protection (SC) family of NIST security controls.

b. Annual assessment of the Agency common security control SC-1 by the Information System Owner (ISO) as part of the system Continuous Monitoring requirement.

P.6 CANCELLATION

a. The next version of NPR 2810.1 cancels this NITR.

Bobby L. German
Chief Information Officer (Acting)

3/11/09
Date

1.0 REQUIREMENT

1.1 System and Communication Protection Policy

1.1.1 The NASA information and information system and communication protection policy shall be consistent with applicable laws, executive orders, directives, regulations and guidance. The objective is to assure effective access control and user accountability to prevent unauthorized access to NASA information or information systems.

1.1.2 NASA shall ensure that information and information systems are adequately protected against potential risks and compromise of sensitive information.

1.1.3 FIPS 140-2 compliant encryption shall be used and implemented for NASA systems in accordance with NPR 2810.1A, Security of Information Technology, paragraph 11.3.15.

1.1.4 NIST 800-30, Risk Management Guide for Information Systems, shall be used for information and information system risk assessments.

1.1.5 NIST 800-21, Guideline for implementing Cryptography in the Federal Government, shall be used in determining the encryption level, strength, and type and be based upon a risk and cost assessment.

1.1.6 NASA mission operations and support systems shall meet the specific encryption requirements as identified in NPR 2810.1A, Security of Information Technology, paragraph 11.3.15.

1.1.7 Domain Name System Security (DNSSEC) shall be employed for all NASA information systems to provide cryptographic protections for DNS communication exchanges.

1.1.7.1 The guidelines of NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide, shall be used for secure domain name system deployment.

1.2 Procedures

1.2.1 The ISO shall:

a. Ensure implementation of the above policies and requirements and the requirements of the NIST SP 800-53 SC-2 through SC-23 Security controls during the life cycle of their information system.

b. Prepare information system and communication protection procedures implementing the above policy and requirements and document the procedures in the System Security Plan (SSP).

c. Assure the requirements of the NASA Organizational Defined Values for the NIST System and Communication Protection security controls are implemented and included in the system and communication protection documentation. Appendix C is an extract of The NASA Organizational Defined Values showing those required values for the System and Communication Protection family of controls.

1.2.2 The Senior Agency Information Security Officer (SAISO) shall:

a. Annually review and update, as required, the Agency System and Communication Protection Policy and Procedures as part of the annual review of the SC-1 control as an Agency common control.

b. Annually certify the SC-1 Agency common control to assure it satisfies the purpose, scope, and compliance requirements for system and communication protection.

c. Provide the Agency patch management capability, resources and oversight for the Agency Patch Selection and Reporting program.

APPENDIX A. Definitions

Term	Definition
Certification	A confirmation in formal documentation that an accepted standard has been met.
Common Control	A security control that is inherited by an information system.
Common Security Control	Security control that can be applied to one or more NASA information systems and has the following properties: (1) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (2) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control may have been applied.
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. (NIST; CNSS 4009, Adapted)
Senior Agency Information Security Officer	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544] Synonymous with Chief Information Security Officer (CISO)
Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]

APPENDIX B. Acronyms

AO	Authorizing Official
DNS	Domain Name System
DNSSEC	Domain Name System Security
FIPS	Federal Information Processing Standards
ISO	Information System Owner
IT	Information Technology
NIST	National Institute of Standards and Technology
NITR	NASA Information Technology Requirement
NPR	NASA Procedural Requirements
OCIO	Office of the Chief Information Officer
SAISO	Senior Agency Information Security Officer
SC	System and Communications Protection (A NIST family of security controls)
SP	Special Publication
SSP	System Security Plan

APPENDIX C. Organization Defined Values for the System and Communication Protection (SC) Security Controls

NASA Organizational Defined Values for NIST SP 800-53 (Rev 2) - System and Communication Protection Security Controls -				
Control	**NIST 800-53 Security Control**	**Value for Low**	**Value for Moderate**	**Value for High**
SC-5	List the types of denial of service attacks or reference a source for a current list that the IS is protected against	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites	http://www.us-cert.gov and http://www.cert.org/tech_tips/denial_of_service.html websites
SC-10	The length of inactive time before a network disconnects a session [after a period of inactivity]	N/A	30 minutes	30 minutes